Claims

[c1] 1. A method of authorizing access to an item, said method comprising:

receiving a presented password from an entity desiring access to said item;

comparing said presented password with a stored password;

authorizing access if said presented password exactly matches said stored password;

denying access if said presented password fails to exactly match said stored password;

variably incrementing a lockout count if said presented password fails to exactly match said stored password; and

locking out access to said item if said lockout count exceeds a predetermined value,

wherein said variably incrementing process increments said lockout count different amounts depending upon how closely said presented password matches said stored password.

[c2] 2. The method in claim 1, wherein, in said variably incrementing process, said lockout count is incremented a

lesser amount as said presented password matches said stored password more closely and is incremented a greater amount as said presented password matches said stored password less closely.

[c3] 3. The method in claim 1, further comprising determining how closely said presented password matches said stored password by evaluating whether the difference between said presented password and said stored password relates to typographical errors.

[c4] 4. The method in claim 1, further comprising determining how closely said presented password matches said stored password by classifying the difference between said presented password and said stored password into different types of password errors.

[c5] 5. The method in claim 4, wherein said different types of password errors cause said lockout count to be incremented by different values.

[c6] 6. The method in claim 4, wherein said types of password errors comprise missing characters, extra characters, transposed characters, and incorrect case usage.

[c7] 7. The method in claim 1, wherein said denying process allows additional passwords to be presented and said locking out process prevents additional passwords from

being presented.

[c8] 8. A method of authorizing access to an item, said method comprising:

receiving a presented password from an entity desiring access to said item;

comparing said presented password with a stored password;

authorizing access if said presented password exactly matches said stored password;

denying access if said presented password fails to exactly match said stored password;

variably incrementing a lockout count if said presented password fails to exactly match said stored password; and

locking out access to said item if said lockout count exceeds a predetermined value,

wherein said variably incrementing process does not increment said lockout count if said presented password is the same as a previously presented password that was entered within a predetermined previous time period.

[c9] 9. The method in claim 8, wherein, wherein said variably incrementing process increments said the lockout count different amounts depending upon how closely said presented password matches said stored password, such

that said lockout count is incremented a lesser amount as said presented password matches said stored password more closely and is incremented a greater amount as said presented password matches said stored password less closely.

[c10] 10. The method in claim 9, further comprising determining how closely said presented password matches said stored password by evaluating whether the difference between said presented password and said stored password relates to typographical errors.

[c11] 11. The method in claim 9, further comprising determining how closely said presented password matches said stored password by classifying the difference between said presented password and said stored password into different types of password errors.

[c12] 12. The method in claim 11, wherein said different types of password errors cause said lockout count to be incremented by different values.

[c13] 13. The method in claim 11, wherein said types of password errors comprise missing characters, extra characters, transposed characters, and incorrect case usage.

[c14] 14. The method in claim 8, wherein said denying process allows additional passwords to be presented and said

locking out process prevents additional password from being presented.

[c15] 15. A method of authorizing access to an item, said method comprising:

allocating a plurality of passwords to a user, wherein each of said passwords has a different expiration date; and

allowing access to said item when said user supplies any one of said passwords before the password supplied has expired.

[c16] 16. The method in claim 15, further comprising notifying said user when each password expires.

[c17] 17. The method in claim 15, further comprising:

allocating additional passwords to said user; and

requiring that an expiration date for said additional passwords be different than expiration dates for any other passwords.

[c18] 18. The method in claim 17, further comprising resetting said expiration dates such that said expirations dates are evenly spaced in time.

[c19] 19. The method in claim 18, wherein if, during said process of allowing access, said user enters an expired password prior to entering an unexpired password, said

method further comprises notifying said user that said expired password has expired, after said user has entered said unexpired password.

[c20] 20.The method in claim 15, wherein said allocating is done at the request of at least one of said user, said item, and a third party.

[c21] 21. The method in claim 15, wherein during said allocating process, said passwords are selected by at least one of said user, said item, and a third party.

[c22] 22. A method of authorizing access to an item, said method comprising:

allocating a plurality of the same passwords to a plurality of users who share the same userid, wherein each of said passwords has a different expiration date; and

allowing access to said item when any of said users supplies any of said passwords before the password supplied has expired.

[c23] 23. The method in claim 22, further comprising notifying all of said users when each password expires.

[c24] 24. The method in claim 22, further comprising:

allocating additional passwords to said users; and

requiring that an expiration date for said additional passwords be different than expiration dates for any other passwords.

[c25] 25. The method in claim 24, further comprising resetting said expiration dates such that said expirations dates are evenly spaced in time.

[c26] 26. The method in claim 25, wherein if, during said process of allowing access, one user of said users enters an expired password prior to entering an unexpired password, said method further comprises notifying said user that said expired password has expired after said user has entered said unexpired password.

[c27] 27. The method in claim 22, wherein said allocating is done at the request of at least one of:

one of said users;
said item; and
a third party.

[c28] 28. The method in claim 22, wherein during said allocating process, said passwords are selected by at least one of:

one of said users;
said item; and
a third party.

[c29] 29. A method of authorizing access to an item, said

method comprising:

allocating the same password to a plurality of users who share the same userid, wherein said password has an expiration date;

allowing access to said item when any of said users supply said password before said password has expired;

mapping information associated with said users to said password in a data file; and

periodically updating said data file.

[c30] 30. The method in claim 29, further comprising notifying said users of expiration of said password a predetermined period before said password expires.

[c31] 31. The method in claim 29, further comprising periodically contacting said users to confirm accuracy of said information within said data file.

[c32] 32. The method in claim 29, wherein said information associated with said users identifies third parties responsible for said users, and

wherein said method further comprises notifying at least one corresponding third party if said user is denied access to said item because of an invalid password.

[c33] 33. The method in claim 29, wherein said users comprise individuals, applications, and application owners.

[c34] 34. The method in claim 29, further comprising updating said data file as said password is changed by said users in said userid.

[c35] 35. The method in claim 29, further comprising checking for inconsistencies between a password being maintained by a user and a password within said data file; and correcting one of user data and said data file when said inconsistencies are found.

[c36] 36.A program storage device readable by machine, tangibly embodying a program of instructions executable by said machine to perform a method of authorizing access to an item, said method comprising:

receiving a presented password from an entity desiring access to said item;

comparing said presented password with a stored password;

authorizing access if said presented password exactly matches said stored password;

denying access if said presented password fails to exactly match said stored password;

variably incrementing a lockout count if said presented password fails to exactly match said stored password; and

locking out access to said item if said lockout count exceeds a predetermined value,

wherein said variably incrementing process increments said lockout count different amounts depending upon how closely said presented password matches said stored password.

[c37] 37. The program storage device in claim 36, wherein, in said variably incrementing process, said lockout count is incremented a lesser amount as said presented password matches said stored password more closely and is incremented a greater amount as said presented password matches said stored password less closely.

[c38] 38. The program storage device in claim 36, wherein said method further comprises determining how closely said presented password matches said stored password by evaluating whether the difference between said presented password and said stored password relates to typographical errors.

[c39] 39. The program storage device in claim 36, wherein said method further comprises determining how closely said presented password matches said stored password by classifying the difference between said presented password and said stored password into different types

of password errors.

[c40] 40. The program storage device in claim 39, wherein said different types of password errors cause said lock-out count to be incremented by different values.

[c41] 41. The program storage device in claim 39, wherein said types of password errors comprise missing characters, extra characters, transposed characters, and incorrect case usage.

[c42] 42. The program storage device in claim 36, wherein said denying process allows additional passwords to be presented and said locking out process prevents additional passwords from being presented.